AMENDMENTS IN THE SPECIFICATION

Please replace the paragraph [0001] with the following:

The present invention is related to the subject matter of the following commonly assigned, copending United States patent application: Serial No. 10/749,261 (Docket No. RPS920030206US2) entitled "Method for Securely Creating An Endorsement Certificate Utilizing Signing Key Pairs" and filed December 31, 2003.

Please replace paragraph [0006] with the following:

With the need for reliable implementation of certificate creation within computer systems permeating the industry, the trusted platform module (tpm) to implement the specification of the trusted computing platform group (tcg). The tpm is a chip that is manufactured to provide the encryption functionality in a trusted device, which is manufactured by a trusted source. The specification of the tcg and tpm are available on the web at ".org" internet address "trustedcomputinggroup".

Please replace paragraph [0007], with the following:

A TPM vendor is required to implement a part that is ~~complaint~~ compliant with the TCG main specification. An OEM of a system that has a TCG complaint part must go to further steps to create a Platform Credential that, in part, contains information about the Endorsement key in the TPM. The actual creation time of the Endorsement key is not important, but it is important that this key be created if a Platform Credential is to be created by the OEM. Since the platform is only in a controlled environment up until it leaves its manufacturing facility, this is when the credential should be created so that the OEM has a level of assurance that any credential it is signing is indeed for a platform created within its secured environment.

Please replace paragraph [0009], with the following:

The manufacturer of the TPM signs a certificate that is physically associated with the TPM. This certificate is tied to the public portion of the endorsement key, and together they confirm that the public key is the endorsement key of this particular TPM. The certificate generation mechanism is required to show public certification of the keys so the users can feel confident that the systems are indeed secure. Thus, there is great value in having the certificate that says that the public key was generated inside of a TPM.

Please replace paragraph 46, beginning on page 1, line 4, with the following:

In one embodiment, the credential server is an on-site, highly protected, FIPS-4, RSA engine (e.g., 4758 processor), which provides high-performance, very secure crypto processing. The RSA engine also knows the 20-byte secret number and any necessary revocation data about the shared secret numbers. FIPS (or Federal Information Processing Standards) is known in the art and the specification may be found at Internet site "csrc.nist.gov/publications/fips".

Please replace paragraph 52, beginning on page 1, line 4, with the following:

It is important to note that while the present invention has been described in the context of a fully functional data processing system, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally, regardless of the particular type of signal bearing media utilized to actually carry out the distribution. Examples of computer readable media include: nonvolatile, hard-coded type media such as Read Only Memories (ROMs) or ~~Erasable, Electrically~~ Electrically Erasable Programmable Read Only Memories (EEPROMs), recordable type media such as floppy disks, hard disk drives and CD-ROMs, and transmission type media such as digital and analog communication links.